#2

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

January 22, 2001

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Kotaro NAGAHAMA
TERMINAL CERTIFICATION SYSTEM AND
METHOD OF CERTIFYING THE SAME
Our Ref. Q62489

Dear Sir:

Attached hereto is the application identified above including 25 sheets of the specification, including the claims and abstract, 11 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney.

The Government filing fee is calculated as follows:

Total claims	16	-	20	=		x	$18.00	=	$.00
Independent claims	3	-	3	=		x	$80.00	=	$.00
Base Fee									$710.00
TOTAL FILING FEE									**$710.00**
Recordation of Assignment									$40.00
TOTAL FEE									**$750.00**

Checks for the statutory filing fee of $710.00 and Assignment recordation fee of $40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from January 25, 2000 based on Japanese Application No. 2000-15670. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: _____
J. Frank Osha
Registration No. 24,625

K. NAGAHAMA
1/22/01
Q62489
1 of 1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２５日

出願番号
Application Number: 特願２０００－０１５６７０

出願人
Applicant (s): 日本電気株式会社

２０００年１１月１７日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９５５６２

【書類名】　特許願
【整理番号】　66400347
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　永浜　公太郎
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100082935
【弁理士】
【氏名又は名称】　京本　直樹
【選任した代理人】
【識別番号】　100082924
【弁理士】
【氏名又は名称】　福田　修一
【選任した代理人】
【識別番号】　100085268
【弁理士】
【氏名又は名称】　河合　信明
【手数料の表示】
【予納台帳番号】　008279
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【包括委任状番号】　9115699

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　認証システムおよびその方法

【特許請求の範囲】

【請求項１】　複数の端末と、これら複数の端末が接続される接続装置とを有して構成される認証システムであって、

前記接続装置および前記複数の端末のそれぞれは、時間に応じてパスワードを変更するパスワードコントローラを有し、

前記接続装置は、前記端末のパスワードコントローラで生成されたパスワードと前記接続装置のパスワードコントローラで生成されたパスワードとが一致する際に、該端末の通信を許可することを特徴とする認証システム。

【請求項２】　前記パスワードコントローラは、複数のパスワードを格納するパスワード格納メモリと、

このパスワード格納メモリに格納された複数のパスワードから１つを選択するパスワード選択回路とを有し、

前記パスワード選択回路は、時間に応じてパスワードの選択を変更することを特徴とする請求項１記載の認証システム。

【請求項３】　前記パスワードコントローラはさらにタイマと、

時刻によっていずれのパスワードを使用するかを示す設定情報を格納する設定メモリとを有し、

前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード選択回路は、前記タイマの示す時間および前記設定情報に従ってパスワードの選択を変更することを特徴とする請求項２記載の認証システム。

【請求項４】　前記接続装置は、前記ネットワークとのフレームの送受信を行うフレーム転送処理部と、

前記端末と接続されて前記端末とフレームの送受信を行う複数のインタフェースと、

前記端末から送信されてくるフレームのパスワードと、前記接続装置の前記パ

スワードコントローラで選択されたパスワードとを比較するパスワード比較器とをさらに有し、

前記インタフェースは、前記パスワード比較器がパスワードの一致を示した場合、対応するフレームを前記フレーム転送処理部へ転送し、不一致を示した場合、対応するフレームを廃棄することを特徴とする請求項１記載の認証システム。

【請求項５】　前記複数の端末はそれぞれ、前記接続装置とのフレームの送受信を制御するフレーム送受信部と、

前記接続装置にフレームを送信する場合に、前記パスワードコントローラからパスワードを受け取り、該パスワードをフレームに付加するフレーム組立部をさらに有することを特徴とする請求項３記載の認証システム。

【請求項６】　前記フレーム組立部は、前記パスワードコントローラからさらにパスワード選択時間を受け取り、前記接続装置に送信するフレームに該パスワードおよびパスワード選択時間を付加することを特徴とする請求項５記載の認証システム。

【請求項７】　前記接続装置のパスワードコントローラは所定の有効時間を格納した有効時間格納メモリをさらに有し、

前記パスワード選択部は、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以内であれば前記パスワード選択時間と前記設定情報とから使用するパスワードを選択し、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以上であれば前記タイマの示す時刻と前記設定情報とから使用するパスワードを選択することを特徴とする請求項６記載の認証システム。

【請求項８】　前記パスワードコントローラは、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリと、

このアルゴリズム格納メモリに格納された複数のパスワード生成アルゴリズムから１つを選択してパスワードを生成するパスワード生成回路とを有し、

前記パスワード生成回路は、時間に応じてパスワード生成アルゴリズムを変更してパスワードを生成することを特徴とする請求項１記載の認証システム。

【請求項９】　前記パスワードコントローラはさらにタイマと、

時刻によっていずれのパスワード生成アルゴリズムを使用するかを示す設定情

報を格納する設定メモリとを有し、

前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード生成回路は、前記タイマの示す時間および前記設定情報に従ってパスワード生成アルゴリズムを選択してパスワードを生成することを特徴とする請求項８記載の認証システム。

【請求項１０】　前記複数のパスワード生成アルゴリズムのそれぞれは、前記タイマの示す時刻に従って異なるパスワードを生成することを特徴とする請求項８記載の認証システム。

【請求項１１】　複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれが時間に応じてパスワードを変更するパスワードコントローラを有するシステムの認証方法であって、

前記接続装置と前記端末との時間を同期させ、

前記端末は、フレームを送信する際に当該端末の前記パスワードコントローラが時間に応じて選択したパスワードをフレームに付加して前記接続装置に送信し、

前記接続装置は、受け取ったフレームに付加されたパスワードと、前記接続装置の前記パスワードコントローラが時間に応じて選択したパスワードとを比較し、

パスワードが一致すれば当該フレームの送信を許可し、一致しなければ当該フレームの送信を許可せず当該フレームを廃棄することを特徴とする認証方法。

【請求項１２】　前記端末は、フレームを前記接続装置に送信する際に、フレームに対して当該端末の前記パスワードコントローラがパスワードを選択した選択時間をさらに付加し、

前記接続装置の前記パスワードコントローラは、前記選択時間に応じてパスワードを選択することを特徴とする請求項１１記載の認証方法。

【請求項１３】　前記パスワードコントローラは、時間に応じて複数のパスワード生成アルゴリズムの中から１つを選択し、該パスワード生成アルゴリズム

によりパスワードを生成することを特徴とする請求項１１記載の認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、システムに接続される端末の認証システムおよびその方法に関する。

【０００２】

【従来の技術】

従来のシステムは、図１７に示されるように、ＬＡＮ（Local Area Network）などのネットワーク４に接続された接続装置１に複数の端末２が接続されて構築されている。この従来のシステムでは、ネットワーク４にアクセス可能な端末の送信元アドレスを管理者があらかじめ接続装置１に登録していた。そして、接続装置１は、登録された送信元アドレスと端末２から送信されてくるフレームの送信元アドレスとを照合することで、当該端末が管理者の許可を受けた端末かどうかを区別していた。

【０００３】

また、従来の他のシステムでは、接続装置１と端末２との双方に特定のパスワードを持たす構成にしていた。この従来の他のシステムでは、まず、端末が特定のパスワードを付加したフレームを送信する。接続装置１は、同じ特定のパスワードと端末２から受け取ったフレームのパスワードとを照合することで端末２のネットワーク４への接続の可否を判断していた。

【０００４】

【発明が解決しようとする課題】

しかしながら、上述の従来技術では、侵入者が許可された送信元アドレスやパスワードを盗用することにより、あたかも管理者から許可を受けた端末２であるかのように見せかけて接続装置１に端末２を接続する恐れがあった。このような場合、接続装置１はその端末２が正しく許可されているものと判断してしまう。このため、不正に接続した端末２がネットワーク４を介して他の端末と通信が成立してしまい、セキュリティが保たれなくなるという問題点があった。

【０００５】

本発明の目的は、このような送信元アドレスやパスワードの盗用による不正アクセスを検出して排除できるセキュリティの高い認証システムを提供することにある。

【０００６】

【課題を解決するための手段】

上記課題を解決するために本発明の認証システムは、複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれは、時間に応じてパスワードを変更するパスワードコントローラを有し、前記接続装置は、前記端末のパスワードコントローラで生成されたパスワードと前記接続装置のパスワードコントローラで生成されたパスワードとが一致する際に、該端末の通信を許可する。

【０００７】

また、前記パスワードコントローラは、複数のパスワードを格納するパスワード格納メモリと、このパスワード格納メモリに格納された複数のパスワードから１つを選択するパスワード選択回路とを有し、前記パスワード選択回路は、時間に応じてパスワードの選択を変更する。

【０００８】

さらに、前記パスワードコントローラはさらにタイマと、時刻によっていずれのパスワードを使用するかを示す設定情報を格納する設定メモリとを有し、前記端末の前記パスワードコントローラの前記タイマは、前記端末が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード選択回路は、前記タイマの示す時間および前記設定情報に従ってパスワードの選択を変更する。

【０００９】

また、前記接続装置は、前記ネットワークとのフレームの送受信を行うフレーム転送処理部と、前記端末と接続されて前記端末とフレームの送受信を行う複数のインタフェースと、前記端末から送信されてくるフレームのパスワードと、前記接続装置の前記パスワードコントローラで選択されたパスワードとを比較する

パスワード比較器とをさらに有し、前記インタフェースは、前記パスワード比較器がパスワードの一致を示した場合、対応するフレームを前記フレーム転送処理部へ転送し、不一致を示した場合、対応するフレームを廃棄する。

【００１０】

さらに、前記複数の端末はそれぞれ、前記接続装置とのフレームの送受信を制御するフレーム送受信部と、前記接続装置に送信するフレーム毎に、前記パスワードコントローラからパスワードを受け取り、該パスワードをフレームに付加するフレーム組立部をさらに有する。

【００１１】

また、前記フレーム組立部は、前記パスワードコントローラからさらにパスワード選択時間を受け取り、前記接続装置に送信するフレームに該パスワードおよびパスワード選択時間を付加する。

【００１２】

さらに、前記接続装置のパスワードコントローラは所定の有効時間を格納した有効時間格納メモリをさらに有し、前記パスワード選択部は、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以内であれば前記パスワード選択時間と前記設定情報とから使用するパスワードを選択し、前記タイマの示す時刻と前記パスワード選択時間との差が有効時間以上であれば前記タイマの示す時刻と前記設定情報とから使用するパスワードを選択する。

【００１３】

また、前記パスワードコントローラは、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリと、このアルゴリズム格納メモリに格納された複数のパスワード生成アルゴリズムから１つを選択してパスワードを生成するパスワード生成回路とを有し、前記パスワード生成回路は、時間に応じてパスワード生成アルゴリズムを変更してパスワードを生成する。

【００１４】

さらに、前記パスワードコントローラはさらにタイマと、時刻によっていずれのパスワード生成アルゴリズムを使用するかを示す設定情報を格納する設定メモリとを有し、前記端末の前記パスワードコントローラの前記タイマは、前記端末

が前記接続装置に接続された際に、前記接続装置の前記パスワードコントローラの前記タイマに同期され、前記パスワード生成回路は、前記タイマの示す時間および前記設定情報に従ってパスワード生成アルゴリズムを選択してパスワードを生成する。

【００１５】

また、前記複数のパスワード生成アルゴリズムのそれぞれは、前記タイマの示す時刻に従って異なるパスワードを生成する。

【００１６】

さらに、本発明における認証方法は、複数の端末と、これら複数の端末が接続される接続装置とを有して構成され、前記接続装置および前記複数の端末のそれぞれが時間に応じてパスワードを変更するパスワードコントローラを有するシステムの認証方法であって、前記接続装置と前記端末との時間を同期させ、前記端末は、フレームを送信する際に当該端末の前記パスワードコントローラが時間に応じて選択したパスワードをフレームに付加して前記接続装置に送信し、前記接続装置は、受け取ったフレームに付加されたパスワードと、前記接続装置の前記パスワードコントローラが時間に応じて選択したパスワードとを比較し、パスワードが一致すれば当該フレームの送信を許可し、一致しなければ当該フレームの送信を許可せず当該フレームを廃棄する。

【００１７】

また、前記端末は、フレームを前記接続装置に送信する際に、フレームに対して当該端末の前記パスワードコントローラがパスワードを選択した選択時間をさらに付加し、前記接続装置の前記パスワードコントローラは、前記選択時間に応じてパスワードを選択する。

【００１８】

さらに、前記パスワードコントローラは、時間に応じて複数のパスワード生成アルゴリズムの中から１つを選択し、該パスワード生成アルゴリズムによりパスワードを生成する。

【００１９】

【発明の実施の形態】

次に本発明の認証システムの第１の実施の形態について図面を参照して説明する。

【００２０】

図１を参照すると、本発明の第１の実施の形態は、ネットワーク４に接続された接続装置１と、この接続装置１に接続される複数の端末２によって構成される。接続装置１と各端末２とはそれぞれ伝送媒体３で接続され、既知の標準化団体IEEE802.3で規定されるアクセス方式（CSMA/CD方式）等に従ってフレームの送受信が行われる。また、接続装置１は、ネットワーク４を介して他の接続装置１と相互に接続されており、各端末間の通信を制御する。

【００２１】

尚、接続装置１として、例えば、ハブやスイッチなど等を使用することができる。

【００２２】

また、接続装置１は、パスワードの生成を行うパスワードコントローラ１１、パスワードの比較を行うパスワード比較器１２、ネットワーク４とフレームの送受信を行うフレーム転送処理部１３、および、１つ以上のインタフェース１４を有して構成される。

【００２３】

端末２は、パスワードの生成を行うパスワードコントローラ２１、接続装置１とフレームの送受信を行うフレーム送受信部２２および送信するフレームの組立を行うフレーム組立部２３を有して構成される。

【００２４】

パスワードコントローラ１１は、パスワードを複数保持しており、時刻にしたがって複数のパスワードの中から所定のパスワードを選択して出力する機能を有している。また、パスワードコントローラ２１もパスワードコントローラ１１と同様の構成である。

【００２５】

バスワード比較器１２は、インタフェース１４から送られてくる送信フレームのパスワードと、接続装置１内のパスワードコントローラ１１で選択されたパス

ワードとを比較する。

【００２６】

フレーム転送処理部１３は、ネットワーク４とのフレームの送受信などを行う。

【００２７】

また、フレーム組立部２３は、接続装置１に送出すべきフレームにパスワードを付加する。図２を参照すると、フレーム組立部２３は、パスワードコントローラ２２で選択されたパスワードを、宛先アドレス、送信元アドレスおよびデータ部の先頭に付加してフレーム５を組み立てる。

【００２８】

次に、本発明の接続装置１の各構成要素およびその動作について図面を用いてさらに詳細に説明する。

【００２９】

図３を参照すると、接続装置１のインタフェース１４は、フレームを端末と伝送媒体３を介して送受信するためのフレーム制御部１４１と、フレーム制御部１４１によって受信されたフレームを一時的に保持しておくフレームバッファ１４２とを有して構成されている。

【００３０】

また、パスワードコントローラ１１は、タイマ１１１、アルゴリズム格納メモリ１１２、設定メモリ１１３、パスワード選択回路１１４を有して構成されている。タイマ１１１は、接続装置１における現在時刻を指し示す。パスワード格納メモリ１１２は、複数種のパスワードを格納している。設定メモリ１１３は、図４に示されるように、時刻によっていずれのパスワードを使用するかを示す設定情報６を格納している。パスワード選択回路１１４は、タイマ１１１および設定メモリ１１３の内容によりパスワード格納メモリ１１２から該当するパスワードを選択する。

【００３１】

図５を参照すると、まず、接続装置１のフレーム制御部１４１は、端末２が接続装置１に接続されているか否かを判断する（Ｓ１１）。端末２の接続が確認さ

れると、フレーム制御部１４１は、パスワードコントローラ１１のタイマ１１１から接続装置１の現在時刻を読出し、端末２へと送信する（Ｓ１２）。その後、端末２からフレームが送信されてくるか否かを監視する（Ｓ１３）。端末２からフレームが送信されてくると、フレーム制御部１４１は、送信されてきたフレームに付加されたパスワードをパスワード比較器１２へ、残りのフレーム部分をフレームバッファ１４２へと送信する（Ｓ１４）。パスワード比較器１２は、フレーム制御部１４１からのパスワードと、パスワード選択回路１１４で選択されたパスワードとを比較する（Ｓ１５）。比較の結果、パスワードが一致していれば、フレーム制御部１４１はフレームバッファ１４２に保持されたフレームをフレーム転送処理部１３へと転送する（Ｓ１６）。一方、パスワードが一致しなければ、フレーム制御部１４１は、フレームバッファ１４２に保持されたフレームを廃棄し、端末２にネットワーク４へのアクセスが許可できない旨を通知する（Ｓ１７）。

【００３２】

次に、パスワードコントローラ１１の動作について説明する。図６を参照すると、パスワードコントローラ１１では、パスワード選択回路１１４は、まず、タイマ１１１から現在時刻を受け取り、設定メモリ１１３に格納される設定情報６を参照する（Ｓ２１）。パスワード選択回路１１４は、パスワード格納メモリ１１２から使用すべきパスワードを読出す（Ｓ２２）。パスワード選択回路１１４は、読出したパスワードをパスワード比較器１２へ送出する（Ｓ２３）。

【００３３】

ここで、パスワード選択回路１１４は、選択するパスワードが前回と同じである場合は、パスワード格納メモリ１１２から逐次パスワードを読込むことなく、前回選択したパスワードをそのままパスワード比較器１２へ再送するような構成してもよい。

【００３４】

また、本発明の端末２の各構成要素およびその動作について図面を用いてさらに詳細に説明する。

【００３５】

図７を参照すると、端末２のパスワードコントローラ２１は、接続装置１のパスワードコントローラ１１と同様に構成されており、パスワード格納メモリ２１２および設定メモリ２１３には接続装置１のパスワード格納メモリ１１２および設定メモリ１１３と同一の内容が格納されている。また、パスワード選択回路２１４は、図６に示される接続装置１のパスワード選択回路１１４と同様に動作し、タイマ２１１および設定メモリ２１３の設定情報６から該当するパスワードをパスワード格納メモリからパスワードを選択する。唯一、端末２のタイマ２１１が接続装置１のタイマ１１１と異なる。すなわち、端末２のタイマ２１１は、端末２の現在時刻を保持するものではなく、端末２が接続装置１に接続された際に接続装置１から送信されてくる接続装置１のタイマ１１１が示す時刻が設定される。

【００３６】

次に、端末２のフレーム送受信部２２の動作について説明する。図８を参照すると、端末２が接続装置１に接続されると、まず、端末２のフレーム送受信部２２は、接続装置１から現在時刻を受け取る（Ｓ３１）。フレーム送受信部２２は、接続装置１の現在時刻を受け取ると、端末２のタイマ２１１に時刻を設定し、接続装置１および端末２のタイマ１１１および２１１の同期を図る（Ｓ３２）。フレーム送受信部２２は、タイマ１１１および２１１の同期を取った後、接続装置１に対してフレーム送信があれば（Ｓ３３）、図３に示されるパスワードが付加されたフレーム５をフレーム組立部２３から受け取り、接続装置１へと送出する（Ｓ３４）。

【００３７】

さらに、端末２のフレーム組立部２３の動作について説明する。図９を参照すると、フレーム組立部２３は、図示せぬプロセッサからフレームの送信命令を受け取ると（Ｓ４１）、パスワード生成部２１４からパスワードを取得する（Ｓ４２）。フレーム組立部２３は、フレーム組立部２３は宛先アドレス、送信元アドレスおよびデータ部からなるフレームの先頭に取得したパスワードを付け加える（Ｓ４３）。そして、フレーム組立部２３は、パスワードが付加されたフレーム５をフレーム送受信部２２へ送出する（Ｓ４４）。

【００３８】

このように、本発明においては、パスワード生成回路で使用するｐすわーどを変化させる。したがって、あるパスワードが解読されるなどして漏洩した場合でも、本発明は時間の経過に伴ってパスワードが変更されるため不正アクセスを検出してネットワークへの接続を不許可にすることができ、ネットワークの高いセキュリティーを実現できる。

【００３９】

次に、本発明の第１の実施の形態の動作について説明する。

【００４０】

図１および図１０を参照すると、まず、接続装置１に端末２が接続されると、接続装置１のタイマ１１１が示す現在時刻を端末２へ送信する（Ｓ１０１）。フレーム送受信部２２は、送信された時刻をタイマ２１１に設定し、接続装置１と同期を図る（Ｓ１０２）。端末２が、接続装置１に対してデータ送信やアクセス要求といったフレームの送信を行う場合には（Ｓ１０３）、端末２のパスワードコントローラ２１が、複数のパスワードの中から現在時刻によって決まるパスワードを選択する（Ｓ１０４）。フレーム組立部２３はパスワードコントローラ２１で選択されたパスワードを付加したフレーム５を組立ててフレーム送受信部２２へ送出する（Ｓ１０５）。フレーム送受信部２２は、パスワードが付加されたフレーム５を伝送媒体３を介して接続装置１へ送出する（Ｓ１０６）。接続装置１のインタフェース１４は、伝送媒体３を介して接続されている端末２からフレーム５を受け取ると、フレーム５からパスワードを読み出してパスワード比較器１２へ送出する（Ｓ１０７）。パスワードコントローラ１１は、複数のパスワードの中から現在時刻によって決まるパスワードを選択する（Ｓ１０８）。パスワード比較器１２は、パスワードコントローラ１１が選択したパスワードと、受信したフレーム５から読み出されたパスワードとを比較する（Ｓ１０９）。比較の結果、パスワードが一致した場合、インタフェース１４はフレーム５を送信してきた端末２がネットワーク４への通信（アクセス）を許可されていると判断し、パスワードを除いたフレームをフレーム転送処理部１３へ送出する（Ｓ１１０）。一方、パスワードが一致しない場合、インタフェース１４は端末２がネットワ

ーク４に不正アクセスしているものと判断し、フレーム転送を不許可として該フレームを廃棄して端末２に通知する（Ｓ１１１）。

【００４１】

尚、パスワードが一致しない場合は、所定の回数だけ再送させる構成としてもよい。

【００４２】

以上のような構成により、不正に入手されたパスワードを用いて不正アクセスが行われたとしても、設定メモリ１１３に定められた時間によるパスワードの変化によって不正アクセスを発見することができ、よりセキュリティーの高い認証システムを提供することが可能となる。

【００４３】

次に、本発明の認証システムの第２の実施の形態について図面を参照して説明する。

【００４４】

この第２の実施の形態においては、端末２のフレーム組立部２３が、図１１に示されるように、パスワードとともにそのパスワードが選択されたパスワード選択時間をフレーム７に付加する構成とする。また、接続装置１では受け取ったフレーム７のパスワード選択時間に従ってパスワードを選択する構成とする。これにより、接続装置１と端末２との間で発生するパスワード選択時間の時間差を無くすことができ、的確なパスワードの比較が行えるようになる。

【００４５】

接続装置１のフレーム制御部１４１は、端末２からフレーム７を受け取ると、フレーム７のパスワードをパスワード比較器１２に、パスワード選択時間をパスワード選択回路１１４に、その他の残りの部分をフレームバッファ１４２に送信する点のみが第１の実施の形態における動作と異なる。その他の動作については図６に示される第１の実施の形態の動作と同様である。

【００４６】

しかしながらこのような構成の場合、パスワードが漏洩した際に端末２から現在時刻を偽ってアクセスされた場合、これを防止することができなくなってしま

う。そこで、このことを考慮して、接続装置１の現在時刻と所定時間以上離れたパスワード選択時間は採用しない構成とする。

【００４７】

図１２を参照すると、接続装置１のパスワードコントローラ１１は、有効時間格納メモリ１１５をさらに有する。この有効時間格納メモリは、パスワード選択時間を有効と判定する有効時間を格納している。

【００４８】

以下に本発明の第２の実施の形態のパスワードコントローラ１１の動作を説明する。

【００４９】

図１３を参照すると、まず、パスワード選択回路１１４は、フレーム制御部１４１からパスワード選択時間を受けると（Ｓ５１）、受け取ったパスワード選択時間とタイマ１１１の示す現在時刻との時間差が有効時間格納メモリ１１５に格納された有効時間以内であるか否かを判定する（Ｓ５２）。もし、パスワード選択時間とタイマの示す現在時刻との差が有効時間以内であれば、パスワード選択回路１１４はパスワード選択時間および設定メモリ１１３の内容から使用すべきパスワードを選択する（Ｓ５３）。一方、パスワード選択時間とタイマの示す現在時刻との差が有効時間以上であれば、パスワード選択回路１１４はパスワード選択時間を採用せず、タイマ１１１の示す現在時刻と設定メモリ１１３の内容から使用すべきパスワードを選択する（Ｓ５４）。パスワード選択回路１１４は、選択したパスワードをフレーム比較器１２へ送出する（Ｓ５５）。

【００５０】

このような構成により、アルゴリズムが変更される時間の前後における通信においても、接続装置１および端末で異なるパスワードが用いられてパスワードが不一致となることがなくなり、的確なパスワードの比較が実現されることになる。

【００５１】

さらに、本発明の認証システムの第３の実施の形態について図面を参照して説明する。

【００５２】

この本発明の第３の実施の形態では、第１の実施の形態におけるパスワードコントローラ１１および２１の構成およびその動作が異なる。その他の構成要素およびそれらの動作については第１の実施の形態と同様である。以下、接続装置１のパスワードコントローラ１１について説明するが、端末２のパスワードコントローラ２１も同様である。

【００５３】

図１４を参照すると、第３の実施の形態におけるパスワードコントローラ１１は、複数のパスワードを格納するパスワード格納メモリ１１２に変えて、複数のパスワード生成アルゴリズムを格納するアルゴリズム格納メモリ１１６を設ける。また、パスワード選択回路１１４に変えて、アルゴリズム格納メモリ１１６から１つのパスワード生成アルゴリズムを読出してパスワードを生成するパスワード生成回路１１７を設ける。さらに、設定メモリ１１３には、図１５に示されるようにパスワード生成回路１１７がパスワード生成アルゴリズムを使用する時間を規定する設定情報８を保持する。

【００５４】

尚、パスワード生成アルゴリズムとしては、分単位程度の時間をパラメータとする一般的な数学による方程式等を利用すればよい。

【００５５】

以下に、本発明の第３の実施例におけるパスワードコントローラ１１の動作について図面を参照して説明する。尚、複数のパスワード生成アルゴリズムは、それぞれ分単位の時間をパラメータとする方程式であるとする。

【００５６】

図１４および図１６を参照すると、まず、パスワード生成回路１１７は、タイマ１１１の現在時刻および設定メモリ１１３の設定情報８を参照して使用するパスワード生成アルゴリズムをアルゴリズム格納メモリ１１６から選択する（Ｓ６１）。パスワード生成回路１１７は、選択したパスワード生成アルゴリズムを使用し、タイマ１１１の現在時刻をパラメータとしてパスワードを生成する（Ｓ６２）。その後、パラメータが変化（時刻の分単位が変化）すると（Ｓ６３）、設

定情報８を参照して使用するアルゴリズムが変更になったか否かを確認する（Ｓ６４）。使用するアルゴリズムが変更された場合は、変更されたパスワード生成アルゴリズムをアルゴリズム格納メモリ１１６から選択し（Ｓ６５）、タイマ１１１の現在時刻をパラメータとしてパスワードを生成する（Ｓ６２へ）。一方、使用するアルゴリズムに変更がなければ、パスワード生成回路１１７は新たなパラメータ（時刻）を用いてパスワードを再生成する（Ｓ６２へ）。

【００５７】

また、さらに、第３の実施の形態に対して、第２の実施の形態で示したパスワード選択時間にかえて、パスワードを生成した時間をパスワード生成時間としてフレームに付加する構成としてもよい。

【００５８】

以上のように、本発明においては、各端末２が接続装置１に接続された際に接続装置１の時刻と同期が取られ、この時刻に合わせてパスワードが変化することになる。したがって、接続装置１と同一のパスワード（または、アルゴリズム）および設定情報を有している正当な端末であれば、接続装置１が時間の経過とともにパスワードを変化させても、接続装置１と同様にパスワードを変化させることができる。よって、設定メモリ１１３および２１３に設定に合わせて異なるパスワードを用いて通信を続行することが可能となる。これに対し、不正に入手したパスワードを利用して通信を行った場合には、時間に伴う接続装置１のパスワードの変化によってパスワード比較器１２がパスワードの不一致を検出し、不正アクセスが発見されることになる。

【００５９】

【発明の効果】

以上の説明で明らかなように、本発明によると、正しいパスワードをフレームに含めて送信できない端末は、接続装置内でフレームを廃棄する。このため、不正な他端末は他の端末との通信が成立しなくなり、ネットワークセキュリティを保つことが可能になる。また、時間の経過とともにパスワードが変更されるため、アナライザ等によってある時点でパスワードが盗まれた（または、解析された）場合においても、盗まれた（解析された）パスワードで継続的に接続装置を介

して通信が行われることを防止することができる。

【図面の簡単な説明】

【図１】

本発明の認証システムの実施の形態を示すブロック図である。

【図２】

本発明で使用されるフレームの構成を示す図である。

【図３】

本発明の接続装置の実施の形態を示す図である。

【図４】

本発明の設定メモリに格納される設定情報を示す図である。

【図５】

本発明の接続装置のフレーム制御部の動作を説明する流れ図である。

【図６】

本発明の接続装置のパスワードコントローラの動作を説明する流れ図である。

【図７】

本発明の端末の実施の形態を示す図である。

【図８】

本発明の端末のフレーム送受信部の動作を説明する流れ図である。

【図９】

本発明の端末のフレーム組立部の動作を説明する流れ図である。

【図１０】

本発明の認証システムの動作を説明する流れ図である。

【図１１】

本発明の第２の実施の形態で使用されるフレームの構成を示す図である。

【図１２】

本発明の第２の実施の形態におけるパスワードコントローラの構成を示す図である。

【図１３】

本発明の第２の実施の形態におけるパスワードコントローラの動作を説明する

流れ図である。

【図１４】

本発明の第３の実施の形態におけるパスワードコントローラの構成を示す図である。

【図１５】

本発明の第３の実施の形態における設定メモリに格納される設定情報を示す図である。

【図１６】

本発明の第３の実施の形態におけるパスワードコントローラの動作を説明する流れ図である。

【図１７】

従来のシステムの概略を示すブロック図である。

【符号の説明】

１　接続装置

２　端末

３　伝送媒体

４　ネットワーク

５、７　フレーム

６、８　設定情報

１１、２１　パスワードコントローラ

１２　パスワード比較器

１３　フレーム転送処理部

１４　インタフェース

２２　フレーム送受信部

２３　フレーム組立部

１１１、２１１　タイマ

１１２、２１２　パスワード格納メモリ

１１３、２１３　設定メモリ

１１４、２１４　パスワード選択回路

１１５　判定条件格納メモリ

１１６　アルゴリズム格納メモリ

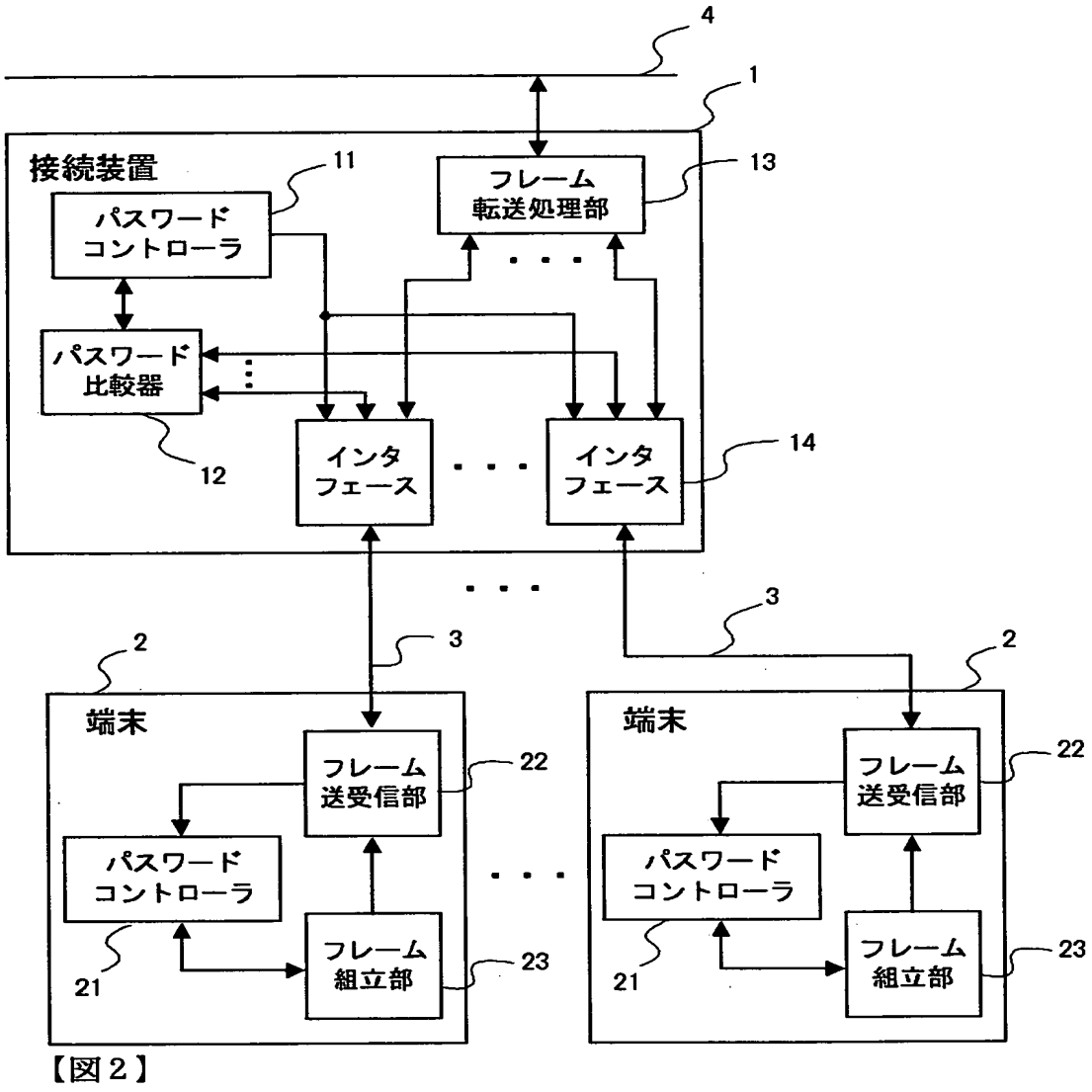
１１７　パスワード生成回路

１４１　フレーム制御部

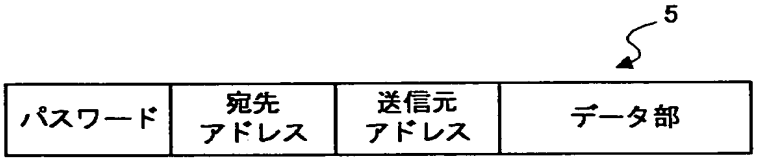
１４２　フレームバッファ

【書類名】　　図面

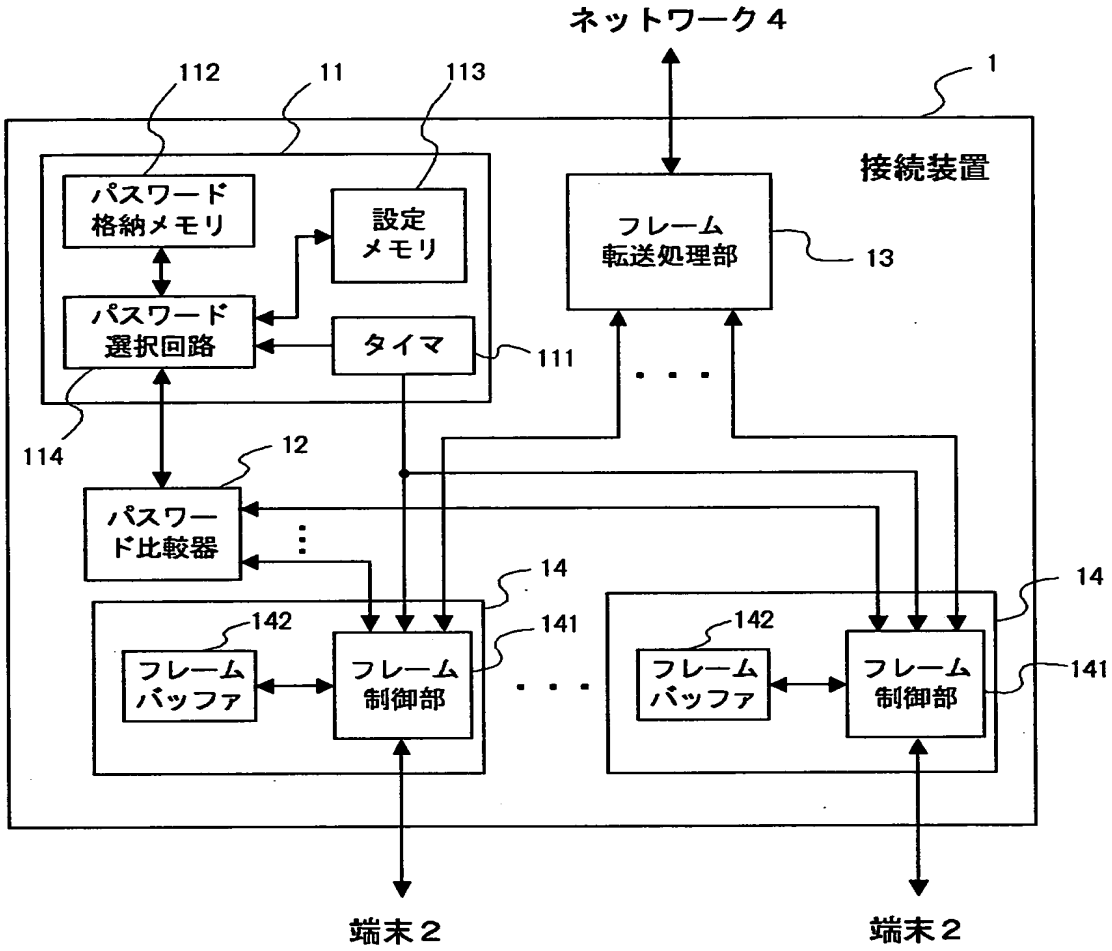
【図１】


4
1
接続装置
11
パスワード
コントローラ
13
フレーム
転送処理部
パスワード
比較器
12
インタ
フェース
インタ
フェース
14
3
2
端末
フレーム
送受信部
22
パスワード
コントローラ
21
フレーム
組立部
23

【図２】


5
パスワード
宛先
アドレス
送信元
アドレス
データ部

【図３】

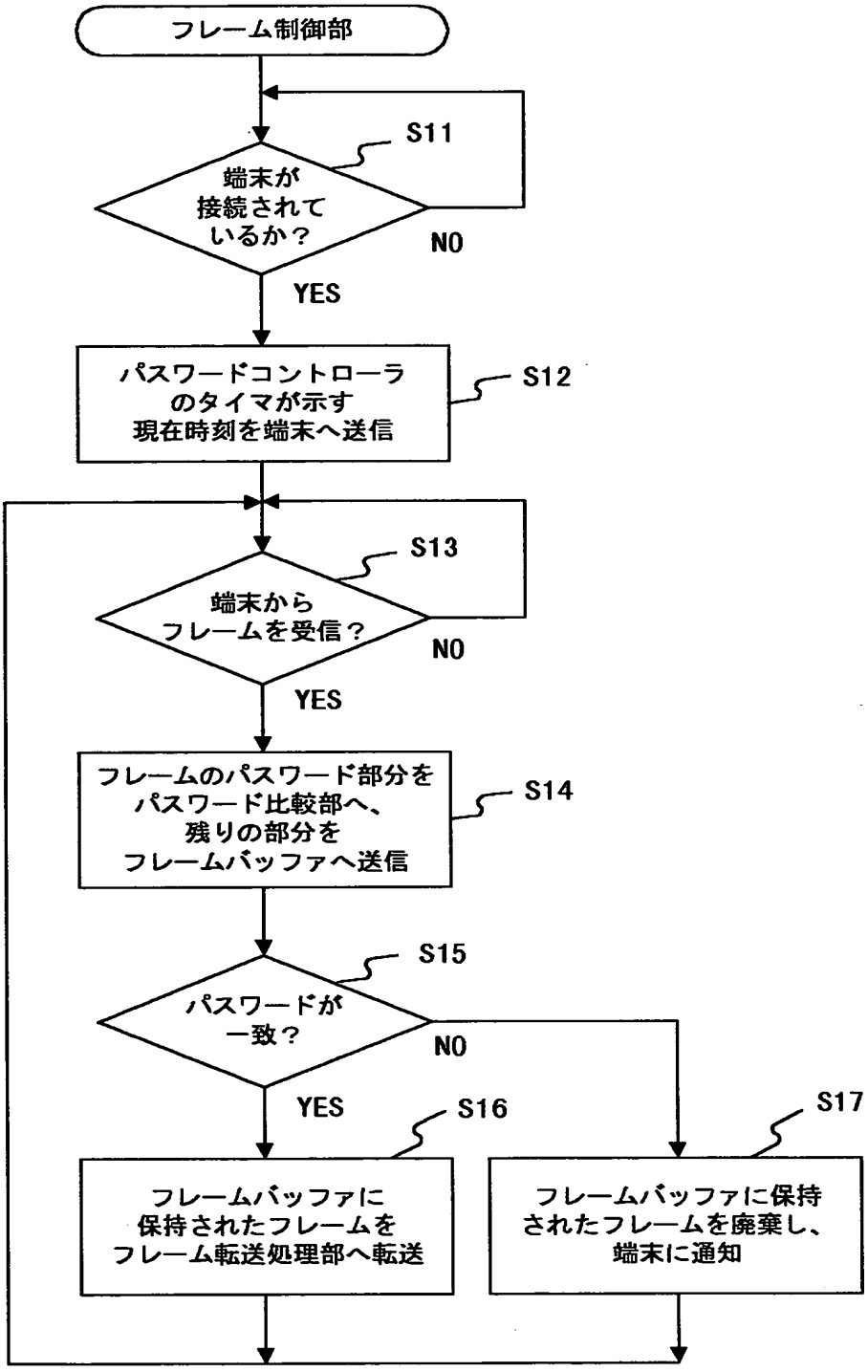


【図４】

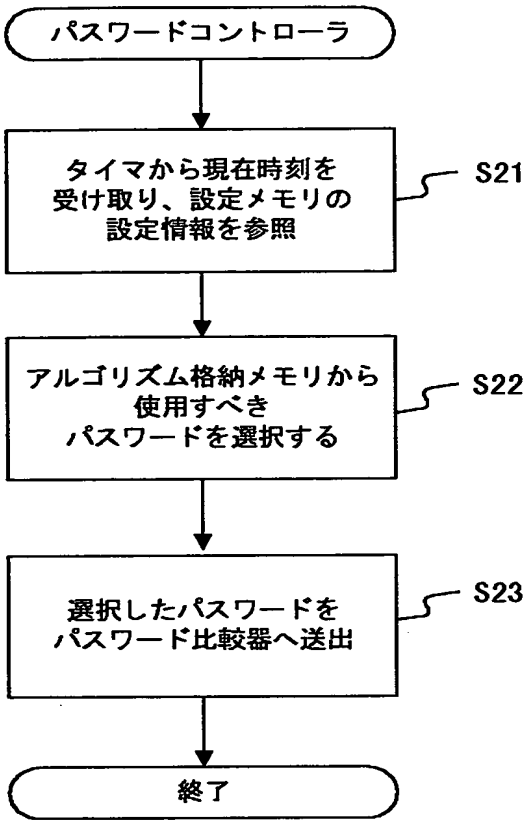
6

時間	使用するパスワード
0:00-0:04	パスワードA
0:05-0:10	パスワードB
⋮	⋮
23:55-23:59	パスワードX

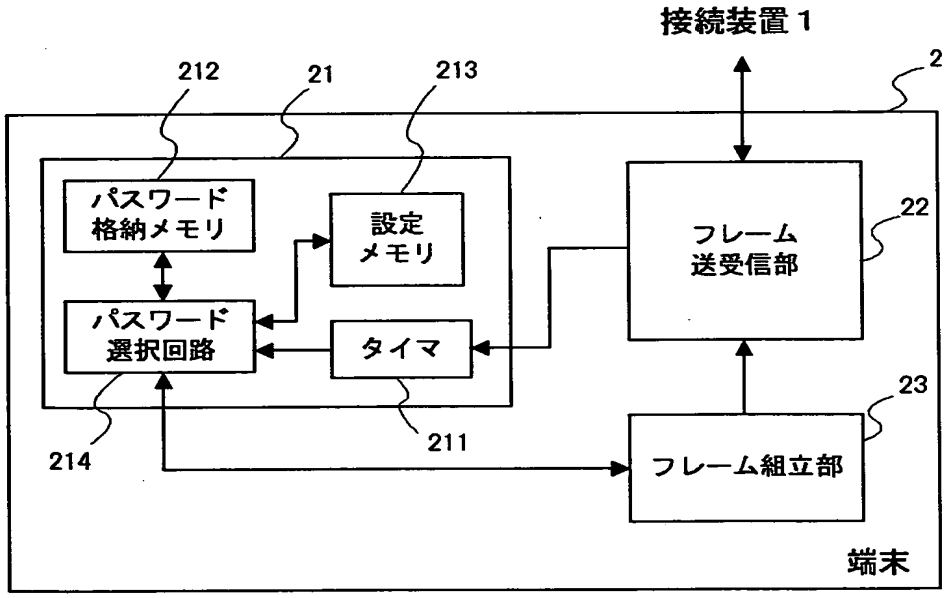
【図５】


フレーム制御部
S11
端末が
接続されて
いるか？
NO
YES
パスワードコントローラ
のタイマが示す
現在時刻を端末へ送信
S12
S13
端末から
フレームを受信？
NO
YES
フレームのパスワード部分を
パスワード比較部へ、
残りの部分を
フレームバッファへ送信
S14
S15
パスワードが
一致？
NO
YES
S16
S17
フレームバッファに
保持されたフレームを
フレーム転送処理部へ転送
フレームバッファに保持
されたフレームを廃棄し、
端末に通知

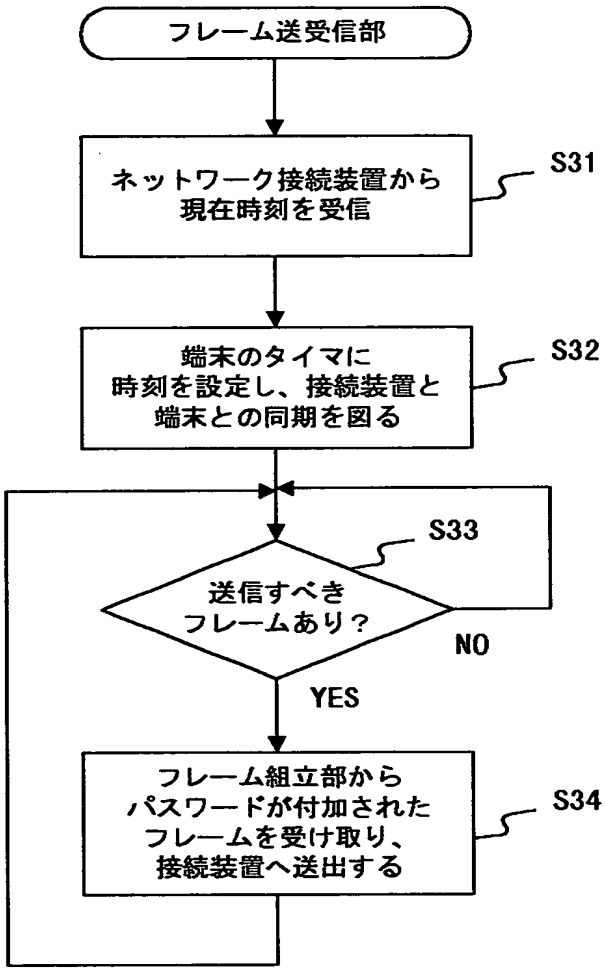
【図６】


パスワードコントローラ
タイマから現在時刻を受け取り、設定メモリの設定情報を参照
S21
アルゴリズム格納メモリから使用すべきパスワードを選択する
S22
選択したパスワードをパスワード比較器へ送出
S23
終了

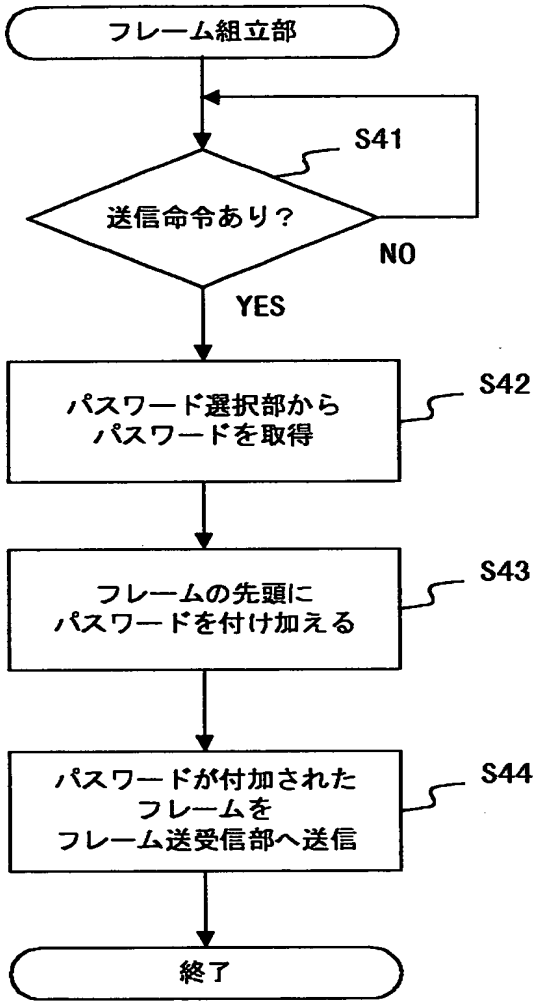
【図７】


接続装置１
2
212
21
213
パスワード格納メモリ
設定メモリ
パスワード選択回路
タイマ
フレーム送受信部
22
23
フレーム組立部
214
211
端末

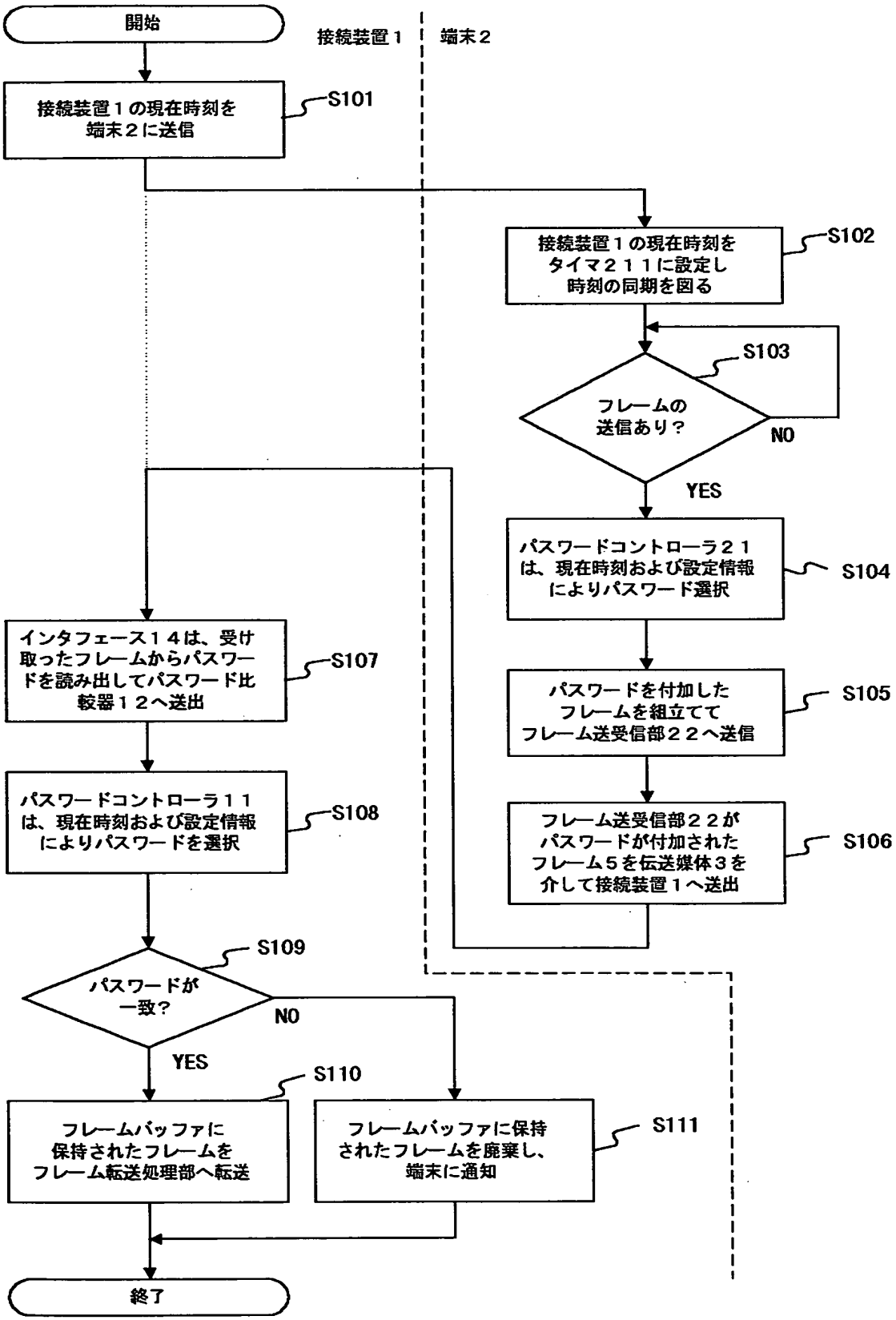
【図８】


フレーム送受信部
ネットワーク接続装置から
現在時刻を受信
S31
端末のタイマに
時刻を設定し、接続装置と
端末との同期を図る
S32
S33
送信すべき
フレームあり？
NO
YES
フレーム組立部から
パスワードが付加された
フレームを受け取り、
接続装置へ送出する
S34

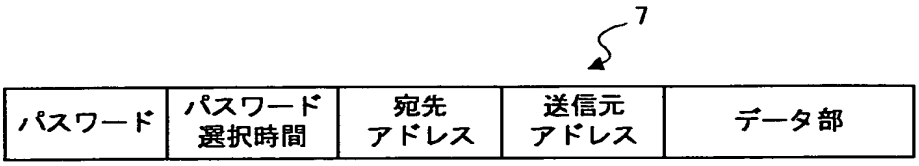
【図９】


フレーム組立部
S41
送信命令あり？
NO
YES
パスワード選択部から
パスワードを取得
S42
フレームの先頭に
パスワードを付け加える
S43
パスワードが付加された
フレームを
フレーム送受信部へ送信
S44
終了

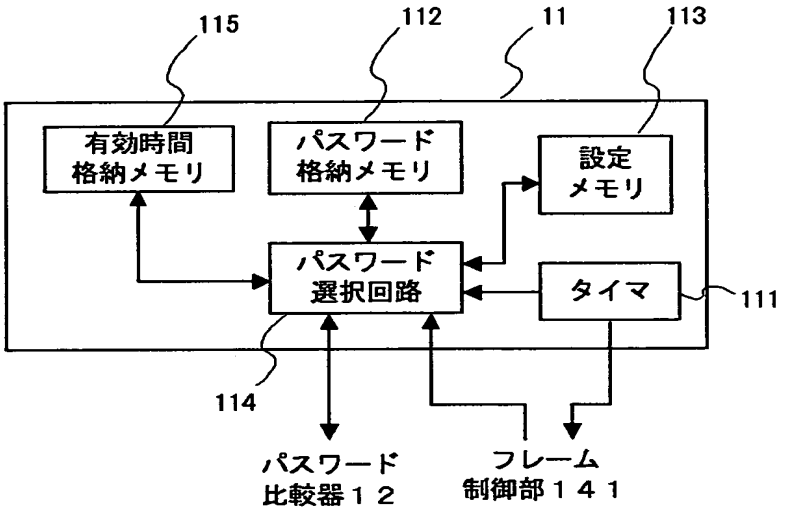
【図１０】


開始
接続装置１
端末２
接続装置１の現在時刻を端末２に送信
S101
接続装置１の現在時刻をタイマ２１１に設定し時刻の同期を図る
S102
S103
フレームの送信あり？
NO
YES
パスワードコントローラ２１は、現在時刻および設定情報によりパスワード選択
S104
パスワードを付加したフレームを組立ててフレーム送受信部２２へ送信
S105
フレーム送受信部２２がパスワードが付加されたフレーム５を伝送媒体３を介して接続装置１へ送出
S106
インタフェース１４は、受け取ったフレームからパスワードを読み出してパスワード比較器１２へ送出
S107
パスワードコントローラ１１は、現在時刻および設定情報によりパスワードを選択
S108
S109
パスワードが一致？
NO
YES
S110
フレームバッファに保持されたフレームをフレーム転送処理部へ転送
フレームバッファに保持されたフレームを廃棄し、端末に通知
S111
終了

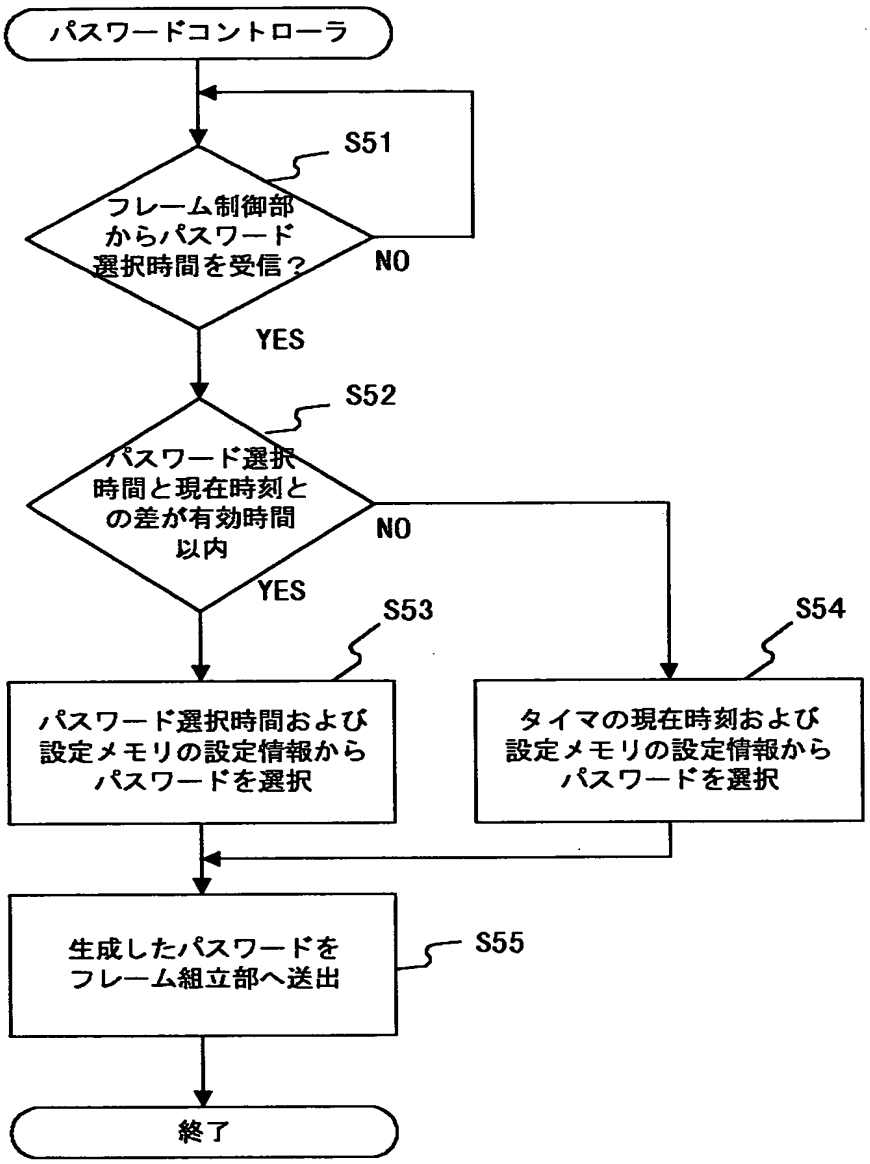
【図１１】


7
パスワード
パスワード
選択時間
宛先
アドレス
送信元
アドレス
データ部

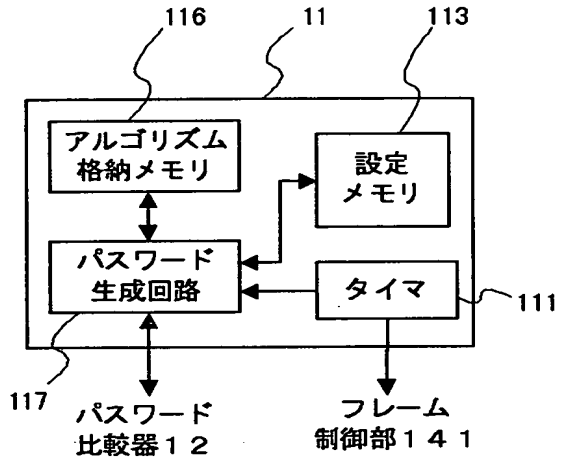
【図１２】


115
112
11
113
有効時間
格納メモリ
パスワード
格納メモリ
設定
メモリ
パスワード
選択回路
タイマ
111
114
パスワード
比較器１２
フレーム
制御部１４１

【図１３】


パスワードコントローラ
S51
フレーム制御部からパスワード選択時間を受信？
NO
YES
S52
パスワード選択時間と現在時刻との差が有効時間以内
NO
YES
S53
パスワード選択時間および設定メモリの設定情報からパスワードを選択
S54
タイマの現在時刻および設定メモリの設定情報からパスワードを選択
生成したパスワードをフレーム組立部へ送出
S55
終了

【図１４】

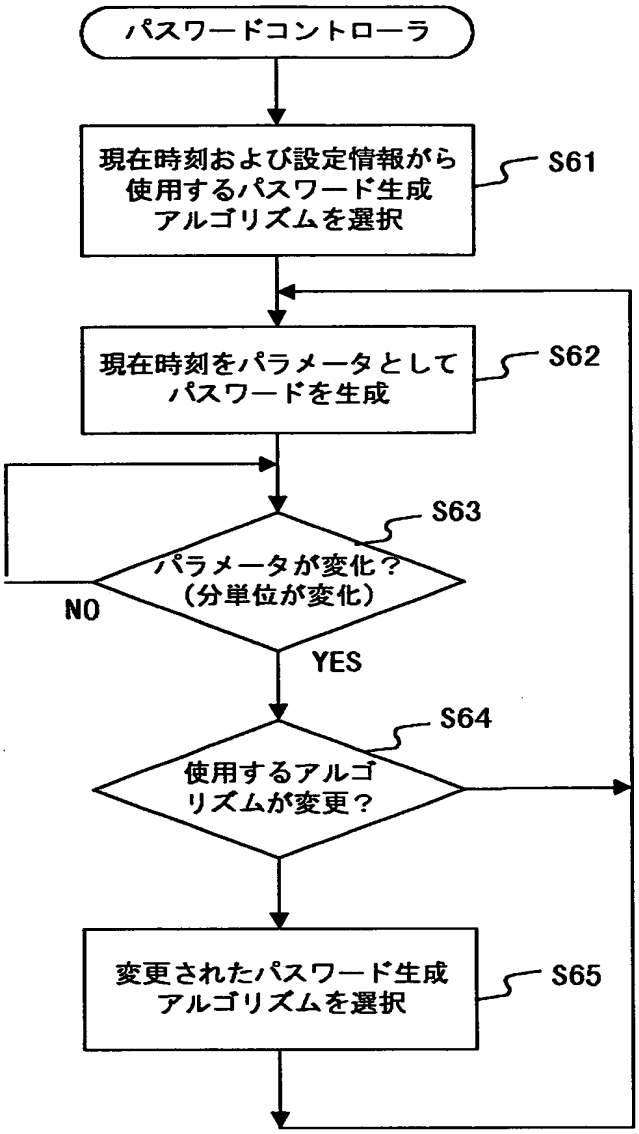


【図１５】

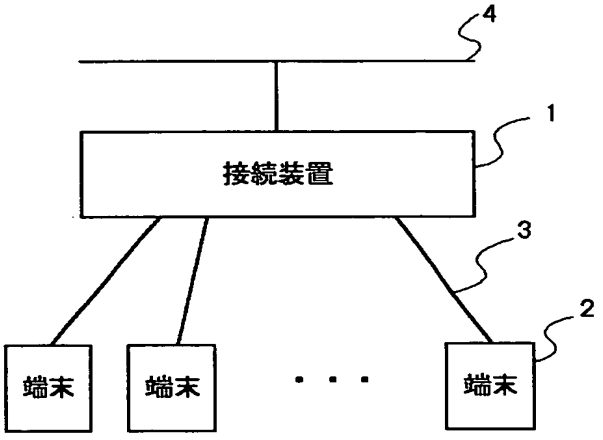
8

時間	使用するアルゴリズム
0:00–0:04	アルゴリズムＡ
0:05–0:10	アルゴリズムＢ
⋮	⋮
23:55–23:59	アルゴリズムＸ

【図１６】


パスワードコントローラ
現在時刻および設定情報がら使用するパスワード生成アルゴリズムを選択
S61
現在時刻をパラメータとしてパスワードを生成
S62
S63
パラメータが変化？（分単位が変化）
NO
YES
S64
使用するアルゴリズムが変更？
変更されたパスワード生成アルゴリズムを選択
S65

【図１７】


4
1
接続装置
3
2
端末
端末
・・・
端末

【書類名】　　要約書

【要約】

【課題】　送信元アドレスやパスワードの盗用による不正アクセスを検出して排除できるセキュリティの高い認証システムを提供する。

【解決手段】　接続装置１および端末２のそれぞれに複数のパスワード（または複数のパスワード生成アルゴリズム）および設定情報を格納する。接続装置１と端末２との時刻を同期させ、設定情報により時間の経過とともにパスワード（またはパスワード生成アルゴリズム）を変更してパスワードを変化させる。端末２は送信するフレームにパスワードを付加して送出し、接続装置１は受け取ったフレームのパスワードと接続装置１のパスワードとを比較する。パスワードが一致した場合、接続装置１は端末２の通信を許可し、一致しない場合には通信を不許可としてフレームを廃棄する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０１５６７０
受付番号	５００００７１００２
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　１月２６日

＜認定情報・付加情報＞

【提出日】　平成12年 1月25日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社